Cyber security

A monitoring tool for governing boards in schools and trusts

Cyber security is the protection of electronic devices, services and networks – and the information on them – from theft or damage.

This tool has been developed to help governing boards monitor their school's/trust's cyber security awareness, controls and response plans, and identify areas for improvement.

Area of focus		Effective practice	Governing board notes and actions
1	Build cyber security awareness	Governing boards can build their own knowledge by: • **Understanding what information, technologies and processes are critical to your organisation** – school leaders should be able to report on this, drawing on expert advice (such as from the data protection officer, IT technician, coordinator or external providers). • **Participating in regular cyber security training** – at least one governor/trustee should complete cyber security training in accordance with the Department for Education's (DfE) cyber security standards. • **Referring to cyber security guidance** such as NCSC's Cyber Security Toolkit for Boards and questions for governors and trustees to ask to improve their understanding.	

Area of focus		Effective practice	Governing board notes and actions
2	Ensure proportionate controls are in place	Cyber security risks should be captured within a risk register or log, control measures identified and referenced in relevant policies and procedures. Governors and trustees should seek assurance that: • **School leaders have drawn on expertise** from within the organisation, and externally where necessary, to identify relevant threats and improve practice. This might include, for example, conducting security audits, encrypting data or implementing multi-factor authentication. • **All types of organisational risks have been evaluated** – for example, premises security (and therefore safeguarding) could be compromised by a cyber attack. NGA's risk management guidance further explains the board's role and the use of a risk register. • **New threats and opportunities are anticipated and identified** as they emerge.	
3	Protect against loss, damage or theft	Governing boards should ensure that their school/trust has adequate insurance in place. The risk protection arrangement (RPA) – the DfE's alternative to commercial insurance – provides cover for cyber incidents, provided that the school has: 1. offline backups 2. undertaken NCSC cyber security training 3. registered with Police CyberAlarm 4. a cyber response plan in place Find out more about cyber security benefits of joining the RPA.	

Area of focus		Effective practice	Governing board notes and actions
4	Evaluate cyber response plans	It is the job of school leaders, working with experts, to construct a robust response plan, setting out the steps that should be taken in the event of a cyber attack, as part of business continuity planning. Seek assurance that plans reflect identified risks and cover: • roles, responsibilities and contact details of key personnel • procedures that staff and others (third parties) should follow • relevant regulatory reporting and legal action The plan should be reviewed regularly, especially after a cyber incident. The NCSC toolkit provides guidance on developing response plans.	
5	Promote vigilance and resilience	Engaged and knowledgeable pupils and staff can be one of the most effective resources in preventing and detecting cyber incidents. This is characterised by: • **a positive cyber security culture** where individuals speak up about potential threats • cyber security **policies and procedures that take into account the way people work** (including working from home or engaging in remote learning, for example) • **cyber security training** to address knowledge gaps specific to your school/trust – NCSC provide training for school staff The NCSC toolkit covers developing a positive cyber security culture.	